
IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

vs.

JEREMY JOHNSON, et al.,

Defendants.

REPORT AND RECOMMENDATION

2:11-CR-501 DN

Chief District Judge David Nuffer

Magistrate Judge Paul M. Warner

Chief District Judge David Nuffer referred this case to Magistrate Judge Paul M. Warner pursuant to 28 U.S.C. § 636(b)(1)(A).¹ On August 13, 2015, Jeremy Johnson filed a sealed motion for a protective order requesting, inter alia, a hearing regarding certain emails that were the subject of a search warrant issued to Google.² The court held an evidentiary hearing on October 29, 2015, and ordered briefing on the matter.³

On November 11, 2015, Mr. Johnson filed a motion to dismiss the indictment for violations of his Sixth Amendment right to effective assistance of counsel.⁴ On December 2, 2015, the United States of America (“Government”) filed a response to Mr. Johnson’s motion.⁵

¹ See docket no. 136.

² See docket no. 595.

³ See docket no. 709.

⁴ See docket no. 753.

⁵ See docket no. 777.

And, on December 8, 2015, Mr. Johnson filed his reply brief.⁶ Judge Nuffer referred this motion to Magistrate Judge Warner under 28 U.S.C. § 636(b)(1)(B).⁷ The court has carefully reviewed and considered the written memoranda submitted by the parties as well as the evidence and testimony presented at the hearing. Now being fully advised, the court issues the following Report and Recommendation.

BACKGROUND

Mr. Johnson is the former president and owner of the now-defunct iWorks, Inc. On December 21, 2010, the Federal Trade Commission (“FTC”) brought a civil complaint against Mr. Johnson, iWorks, Inc., and many others.⁸ The FTC complaint alleged, inter alia, that the defendants made various misrepresentations and engaged in deceptive and unfair practices in the course of conducting iWorks’s business.⁹ A criminal investigation was opened, and on June 10, 2011, Mr. Johnson was charged by felony complaint with a single count of Mail Fraud, in violation of 18 U.S.C. § 1341.¹⁰ He was arrested the following day and indicted on June 16, 2011.¹¹ He first appeared before this court on July 7, 2011, and Nathan A. Crane was appointed as his counsel.¹²

⁶ See docket no. 813.

⁷ See docket no. 784.

⁸ See *Federal Trade Commission v. Jeremy Johnson, et al.*, No. 2:10-cv-02203 (D. Nevada) (hereinafter “FTC docket no. ___”).

⁹ See FTC docket no. 1.

¹⁰ See docket no. 1.

¹¹ See docket no. 2.

¹² See docket no. 7.

Mr. Crane represented Mr. Johnson until February 1, 2013.¹³ The pair communicated extensively by email regarding the criminal case.¹⁴ Mr. Johnson used the email addresses royalorangecat@gmail.com and evilorangecat22@gmail.com to communicate with counsel.¹⁵ On February 1, 2013, after Mr. Crane withdrew, Ronald J. Yengich and Chelsea Koch were appointed to serve as Mr. Johnson's counsel,¹⁶ and Mr. Johnson began to communicate with his new defense team using email.

On March 6, 2013, the Government filed a First Superseding Indictment against Mr. Johnson and the other defendants setting forth 86 various counts, including: Conspiracy, False Statement to Bank, Wire Fraud, Bank Fraud, Participating in Fraudulent Banking Activities, Conspiracy to Commit Money Laundering, Money Laundering, and Aiding and Abetting.¹⁷ Much of the evidence the Government relied on to support the allegations in the First Superseding Indictment was obtained from FTC files, provided in response to a production letter or pursuant to grand jury subpoena. The Government also obtained additional evidence from businesses associated with iWorks, including business records and banking records obtained pursuant to subpoenas issued by the Grand Jury. The Grand Jury subpoenaed records from Wells Fargo, Cardflex, Mach I, various banks and other businesses that had conducted transactions related to iWorks merchant bank accounts and the charges in the Indictment. On

¹³ See docket no. 196.

¹⁴ See docket no. 753, Exhibit 1.

¹⁵ See *id.*

¹⁶ See docket no. 196.

¹⁷ See docket no. 211.

December 5, 2013, the Government filed a Second Superseding Indictment that made only minor and technical changes.¹⁸ On August 5, 2015, the Government filed a Third Superseding Indictment.¹⁹ The Third Superseding Indictment includes the exact same 86 counts as the First Superseding Indictment. The substantive changes from the First and Second Superseding Indictments to the Third Superseding Indictment are minimal.

Sometime in early 2013, the Government opened an investigation into allegations against Mr. Johnson regarding witness tampering and obstruction of justice. As part of their investigation, the Government sought to seize the contents of Mr. Johnson's Google email accounts royalorangecat@gmail.com and evilorangecat22@gmail.com. The warrant and affidavit were based on allegations that Mr. Johnson and two other named individuals, personally contacted and tampered with two witnesses in this case and that Mr. Johnson had used these two Google email accounts to do so.²⁰

The Google search warrant sought all emails between the specific witnesses and Mr. Johnson from January 1, 2011 until the day the warrant was issued.²¹ Google was required to produce the following information:

The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail²²

¹⁸ See docket no. 341.

¹⁹ See docket no. 584.

²⁰ See docket no. 777, Exhibit 2.

²¹ See docket no. 777, Exhibit 1.

²² *Id.*

The specific information that was to be seized by the government:

All information . . . that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. § 1512(b), those violations involving Jeremy Johnson . . . and others and occurring after January 1, 2011, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Information related to communications between Jeremy Johnson . . . and/or others regarding contacting any witness or potential witness in the criminal or civil case. In addition, information related to communications between Jeremy Johnson . . . and/or other witness in the criminal or civil matter.

b. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts. Information relating to who communicated with the account is limited to information that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. § 1512(b).²³

On June 27, 2013, Google responded to the warrant by providing two discs containing electronic data to Special Agent (“SA”) Jason Henrikson from the Federal Bureau of Investigation (“FBI”).²⁴ SA Henrikson inserted the discs into his computer and opened “a few of the files to verify that the contents of the discs were readable,” but he does not “recall the contents of the files” he opened.²⁵ He informed Assistant United States Attorney (“AUSA”) Karin Fojtik that he had received the discs from Google.²⁶ She suggested that SA Henrikson filter the contents of the discs for privileged communications prior to his review.²⁷

²³ Docket no. 777, Exhibit 1 (names of third persons appearing in the warrant omitted).

²⁴ See docket no. 753, Exhibit 3.

²⁵ Docket no. 753, Exhibit 3.

²⁶ See *id.*

²⁷ See *id.*

SA Henrikson contacted FBI SA Randy Kim of the Intermountain West Regional Computer Forensics Lab (“RCFL”) to verify that SA Kim could filter emails containing specific names before SA Henrikson conducted his review.²⁸ SA Kim confirmed the e-mails could be filtered.²⁹ On August 8, 2013, SA Henrikson provided to SA Kim a list of attorneys “known to have possible affiliation with the Jeremy Johnson case” generated by AUSA Fojtik and AUSA Jason Burt.³⁰ On August 12, 2013, SA Henrikson delivered the discs containing the search warrant production to the RCFL for filtering.³¹ On October 4, 2013, SA Henrikson requested that the names “Ronald Yengich” and “Rodney Snow” be added to the list of filtered attorneys.³²

After receiving the warrant production, SA Kim proceeded to filter emails and other communications containing the names provided by SA Henrikson.³³ The filter captured exact matches; spelling differences and name ordering (e.g. last name first, first name last) could impact whether a communication would be filtered.³⁴ Apparently, several members of Mr. Johnson’s criminal and civil defense teams were not on the list, including Meg Schmitt, a paralegal who worked on Mr. Johnson’s parallel civil defense, and Jeff Wright, an investigator employed by Mr. Yengich for the criminal case.³⁵ A few days later, SA Kim notified SA

²⁸ *See id.*

²⁹ *See id.*

³⁰ *Id.*

³¹ *See id.*

³² *See id.*

³³ *See* docket no. 753, Exhibit 6.

³⁴ *See* Evid. Hr’g Tr. 72, Oct. 29, 2015, (hereinafter, Tr. at ____).

³⁵ *See* docket no. 753 at 6, Exhibit 6.

Henrikson the filter had been completed, and SA Henrikson began reviewing the production.³⁶

SA Henrikson conducted a second filter by performing key word searches relating to possible obstruction or witness tampering charges.³⁷ He stated that he does not recall seeing any communications involving attorneys during his review.³⁸

SA Henrikson completed his review on November 11, 2013, and bookmarked some items relevant to the tampering investigation.³⁹ SA Henrikson then provided those items to AUSA Fojtik for her review.⁴⁰ She estimates that she reviewed fewer than 50 hard-copy pages of emails, all of which were responsive to search terms regarding witness tampering.⁴¹ AUSA Fojtik further stated in her sworn affidavit, “At no point during my review of the emails did I see any materials related to attorney-client communications, nor any emails other than those related to the three individuals, and other associates of Mr. Johnson related to possible witnesses tampering.”⁴²

On November 7, 2013, SA Henrikson retrieved the warrant discs from the RCFL and checked them into the FBI’s evidence control room.⁴³ The unfiltered discs remained with the FBI until sometime in January, 2015, when SA Henrikson retrieved and delivered them to the

³⁶ *See id.*, Exhibit 3.

³⁷ *See id.*

³⁸ *See id.*

³⁹ *See id.*

⁴⁰ *See id.*

⁴¹ *See id.*, Exhibit 2.

⁴² *Id.*

⁴³ *See id.*, Exhibit 3.

United States Attorneys Office at AUSA Fojtik's request.⁴⁴ Copies of the unfiltered discs were made and provided to Chelsea Koch, who was then Mr. Johnson's counsel.⁴⁵ Ms. Koch found that she could not access the data in the format the government provided and delivered it to defense discovery coordinator Eric Wheeler in February 2015.⁴⁶ Mr. Wheeler uploaded the unfiltered Google search warrant production onto the Concordance e-discovery platform and into a searchable database entitled "MBox."⁴⁷

Mr. Johnson apparently reviewed the production and informed new counsel that he located email communications between himself and previous counsel in the MBox database and that he believed other defendants may have access to privileged communications in the emails.⁴⁸ As a precaution, Mr. Johnson's counsel sent a Notice of Inadvertent Disclosure to counsel for all co-defendants.⁴⁹ However, Mr. Wheeler testified at the evidentiary hearing that the MBox database was never accessible by any other defense counsel or their staff.⁵⁰

On July 20, 2015, Johnson filed a sworn affidavit in the FTC civil case signed by Pamela Lindquist, an investigator working for Mr. Yengich and Ms. Koch.⁵¹ Referring to the unfiltered Google materials provided by the United States Attorney's Office to Ms. Koch, Ms. Lindquist

⁴⁴ *See id.*

⁴⁵ *See id.*

⁴⁶ *See* docket no. 777, Exhibit 4.

⁴⁷ *See* docket no. 753, Exhibit 7.

⁴⁸ *See* docket no. 753, Exhibit 8.

⁴⁹ *See id.*

⁵⁰ *See* Tr. at 28.

⁵¹ *See* FTC docket no. 1631, Exhibit 1.

states the following in the last paragraph of her sworn affidavit to the Nevada Court: “I have since confirmed that everyone that has access to the database, all defendants, their lawyers, and defense teams, also has access to these privileged emails.”⁵² However, on October 29, 2015, Ms. Lindquist testified that she did not confirm with every defense counsel that they indeed had access to the MBox, but only that counsel for Scott Leavitt had informed her that he could see the emails.⁵³

DISCUSSION

Mr. Johnson contends that the Government violated his Sixth Amendment right to counsel. Specifically, Mr. Johnson asserts that the Government intentionally and prejudicially intruded upon Mr. Johnson’s attorney-client relationship by knowingly capturing his privileged communications with counsel, failing to acknowledge in the Google search warrant that privileged materials may be captured, and failing to take appropriate measures to screen the prosecution team from privileged information. Mr. Johnson argues that the only remedy for this alleged violation is dismissal of the indictment.

The Sixth Amendment guarantees the right to effective assistance of counsel. *See McMann v. Richardson*, 793 U.S. 759, 751 (1970). The Supreme Court has recognized that the government’s intrusion into the attorney-client relationship may violate a defendant’s Sixth Amendment rights in some situations. *See Weatherford v. Bursey*, 429 U.S. 545, 556-57 (1977).

⁵² *Id.*

⁵³ *See* Tr. at 55.

For instance, in *Shillinger v. Haworth*, the defendant's attorney arranged to hold trial preparatory sessions in the courtroom but because the defendant was incarcerated, a deputy sheriff was present at all times. *See Shillinger*, 70 F.3d 1132, 1134 (10th Cir. 1996). It became obvious during trial that the deputy had been relating privileged information he was privy to from trial preparation sessions to the prosecutor. *See id.* at 1134-35. The Tenth Circuit concluded that the prosecutor violated the defendant's Sixth Amendment rights and remanded the case to the district court for consideration of the appropriate remedy. *See id.* at 1143. In particular, the Tenth Circuit held,

Because we believe that a prosecutor's intentional intrusion into the attorney-client relationship constitutes a direct interference with the Sixth Amendment rights of a defendant, and because a fair adversary proceeding is a fundamental right secured by the Sixth and Fourteenth Amendments, we believe that absent a countervailing state interest, such an intrusion must constitute a per se violation of the Sixth Amendment.

Shillinger v. Haworth, 70 F.3d 1132, 1142 (10th Cir. 1996). The court further clarified that "when the state becomes privy to confidential communications because of its purposeful intrusion into the attorney-client relationship and lacks a legitimate justification for doing so, a prejudicial effect on the reliability of the trial process must be presumed." *Id.* However, it also stated that this per se rule "in no way affects the analysis to be undertaken in cases in which the state has a legitimate law enforcement purpose for its intrusion." *Id.*

Mr. Johnson argues that the Google search warrant and handling of the data produced was an intentional intrusion into his attorney-client relationship and a per se violation of his Sixth Amendment rights under *Shillinger*. Specifically, Mr. Johnson asserts that the Government knew that the data produced by Google would capture his attorney-client communications but it

did not inform the court nor did it implement sufficient procedures to avoid violating Mr. Johnson's Sixth Amendment rights. Moreover, Mr. Johnson argues, the Government lacked a legitimate law enforcement purpose for the intrusion.

The court does not agree. The Google search warrant was used as a legitimate law enforcement tool to investigate potential witness tampering and obstruction of justice charges. There is no evidence to suggest that the Government should have known that the Google search warrant would capture Mr. Johnson's attorney-client communications. Nevertheless, the Government did implement sufficient procedures to ensure that it only examined those documents and emails responsive to its investigation.

District Judge Dale A. Kimball rejected a nearly identical claim in *United States v. Zajac*, No. 2:06CR811DAK, 2008 WL 1808701 (D. Utah April 21, 2008). In that case, the defendant claimed a per se violation of his Sixth Amendment rights when the government obtained jail-house calls he had made to his attorney. *See id.* at *3. The government had obtained a subpoena to gather evidence of calls about incriminating statements the defendant made through jail-house calls. *See id.* Because the Weber County jail did not separate telephone calls, it produced all of the calls the defendant had made in response to the subpoena. *See id.* The United States Attorneys Office and the investigating agents identified the calls the defendant had made to his attorney (no taint team was used), and they "purposefully did not review or listen to the telephone calls made to attorneys because they could have contained attorney-client communications." *Id.* at *4. Then,

to fully comply with discovery rules, the government provided the incriminating calls as well as the other calls made by the defendant. The government provided to [d]efendant's

counsel the entire record in discovery because the jail had provided the entire record to it. While the government took care not to review any privileged material, it did not exclude those potentially privileged conversations from defense counsel when it provided discovery.

Id. This procedure is exactly what occurred in the present case; that is, the Government provided Mr. Johnson's counsel an unfiltered copy of the Google search warrant materials. Unlike the prosecutor in *Shillinger*, the government in *Zajac* had a legitimate purpose for obtaining the jail-house calls and it had taken measures to avoid listening to potentially privileged materials.

Similarly, circumstances in the instant matter are analogous to those in *Zajac*. The Government obtained the Google search warrant materials for a legitimate law enforcement purpose: to investigate allegations by witnesses that they had been personally contacted by Johnson and his associates in an effort to change their prior statements made in connection with the civil and criminal cases. SA Henrikson searched the Google materials for the sole purpose of determining the validity of the witnesses' complaints and whether such contact violated federal law. SA Henrikson submitted two sworn declarations and he testified at an evidentiary hearing during which he was subject to cross-examination by Mr. Johnson's counsel. SA Henrikson has never seen a single privileged document. No other member of the prosecution team has seen the Google materials and no member of the prosecution team has or will use the materials in any way. Like *Zajac*, there has been no "purposeful intrusion" into any privileged materials here.

As Judge Kimball stated in *Zajac*,

Defendant fails to provide any specific communication, transcript, or documentation which demonstrates that the government obtained any evidence or content from these conversations or listened to the conversations. Defendant provides conclusory and speculative accusations that the government engaged in egregious and outrageous illegal

conduct. There are no specific facts to support Defendant's allegations that there was an intrusion of the attorney-client privilege or that such intrusion was purposeful.

Id. at *5. Likewise, this court concludes that Mr. Johnson has failed to demonstrate that the Government's Google search warrant was a purposeful intrusion into attorney-client communications or that it was obtained without a legitimate law enforcement purpose. There is no evidence that the Government viewed any privileged materials. Because Mr. Johnson has failed to show a deprivation of his rights and there is no evidence of wrong-doing, the court finds that there is no basis for dismissing the indictment.

As a final matter, the Government urges this court to rule that Mr. Johnson waived his attorney-client privilege with respect to the documents located in the MBox database. Specifically, the Government asserts that Mr. Johnson either voluntarily provided privileged documents to the other defendants and/or defense counsel or that he inadvertently disclosed the information. The Government relies upon Pamela Lindquist's affidavit and her testimony at the evidentiary hearing that defense counsel accessed the Mbox database. However, Ms. Lindquist's affidavit is replete with errors and her testimony is not credible. Because her testimony conflicts with that of defense discovery coordinator Mr. Wheeler, who testified that the Mbox database was not accessible by any other offices, this court cannot conclude that Mr. Johnson has waived his attorney-client privilege with respect to the contents of the Mbox database.

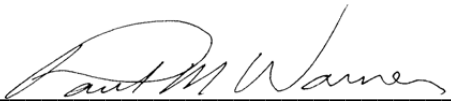
CONCLUSION AND RECOMMENDATION

Based on the foregoing, this court concludes that there has been no violation of Mr. Johnson's Sixth Amendment rights. As such, **IT IS HEREBY RECOMMENDED** that Mr.

Johnson's motion to dismiss⁵⁴ be **DENIED**. Copies of this Report and Recommendation are being sent to all parties, who are hereby notified of their right to object. *See* 28 U.S.C. § 636(b)(1); Fed. R. Civ. P. 72(b). The parties must file any objection to this Report and Recommendation within fourteen (14) days after being served with a copy of it. *See* 28 U.S.C. § 636(b)(1); Fed. R. Civ. P. 72(b). Failure to object may constitute waiver of objections upon subsequent review.

Dated this 12th day of January, 2016.

BY THE COURT:

A handwritten signature in cursive script, appearing to read "Paul M. Warner", is written over a horizontal line.

PAUL M. WARNER
United States Magistrate Judge

⁵⁴ *See* docket no. 753.